CLAIMS

We claim:

1. A method for discouraging a theft of content material comprising:

collecting a plurality of data items comprising the content material to form a data set that is sized to be sufficiently large so as to discourage a subsequent transmission of the data set via a limited bandwidth communications channel,

each of the plurality of data items having an associated security identifier that is configured such that a modification of the data item effects a modification of the security identifier,

creating an entirety parameter based on a plurality of the security identifiers; and

including the entirety parameter in the data set to facilitate a preclusion of processing of a select data item of the plurality of data items in the absence of an entirety of the data set.

2. The method of claim 1, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

3. The method of claim 1, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

4. The method of claim 3, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

5. The method of claim 3, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

6. The method of claim 1, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

7. The method of claim 1, wherein the entirety parameter is bound to a table of contents that is associated with the data set.

8. The method of claim 1, further including:

creating a plurality of other entirety parameters, each of the plurality of other entirety parameters being based on an associated plurality of security identifiers, and

including the plurality of other entirety parameters in the data set to further facilitate a preclusion of processing of each data item in the absence of an entirety of the data set.

9. A method of decoding content material from a source comprising:

reading an entirety parameter corresponding to the content material from the source,

reading a plurality of security identifiers from the source, upon which the entirety parameter is based, each security identifier corresponding to a data item of the content material,

determining an entirety value based on the plurality of security identifiers,

rendering the content material from the source in dependence upon a correspondence between the entirety value and the entirety parameter.

10. The method of claim 9, wherein

reading the entirety parameter includes a random selection from a set of entirety parameters, each entirety parameter of the set of entirety parameters having an associated set of security identifiers.

11. The method of claim 9, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

12. The method of claim 9, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

13. The method of claim 12, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

14. The method of claim 12, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

15. The method of claim 9, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

16. The method of claim 9, wherein the entirety parameter is bound to a table of contents that is associated with the content material.

17. A storage medium that is configured to contain content material, the storage medium comprising

a data structure that includes:

a plurality of data items, each data item having an associated security identifier, and

an entirety parameter that is dependent upon a plurality of the security identifiers; and

wherein

each security identifier of the plurality of security identifiers is configured such that a modification of the data item effects a modification of the security identifier, and

the entirety parameter facilitates a determination of whether an entirety of the plurality of data items is present on a subsequent copy of at least a portion of the plurality of data items.

18. The storage medium of claim 17, further including

a plurality of other entirety parameters, each of the plurality of other entirety parameters being dependent upon an associated plurality of security identifiers.

19. The storage medium of claim 17, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

20. The storage medium of claim 17, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

21. The storage medium of claim 20, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

22. The storage medium of claim 20, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

23. The storage medium of claim 17, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

24. The storage medium of claim 17, wherein the entirety parameter is bound to a table of contents that is associated with the data set.

25. An encoder of content material comprising:

a selector that is configured to select a plurality of data items comprising the content material to form a data set that is sized to be sufficiently large so as to discourage a subsequent transmission of the data set via a limited bandwidth communications channel,

each of the plurality of data items having an associated security identifier that is configured such that a modification of the data item effects a modification of the security identifier,

a binder that is configured to create an entirety parameter based on a plurality of the security identifiers that facilitates a determination of whether an entirety of the plurality of data items is present, and

a recorder that is configured to combine the entirety parameter with the plurality of data items to form a self-referential data set that is stored on a recorded medium.

26. The encoder of claim 25, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

27. The encoder of claim 25, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

28. The encoder of claim 27, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

29. The encoder of claim 27, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

30. The encoder of claim 25, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

31. The encoder of claim 25, wherein

the binder is further configured to bind the entirety parameter to a table of contents that is associated with the data set.

32. The encoder of claim 25, wherein

the binder is further configured to create a plurality of other entirety parameters, each of the plurality of other entire parameters being based on an associated plurality of security identifiers, and

the recorder is further configured to combine the plurality of other entirety parameters with the data set to further facilitate a preclusion of processing of each data item in the absence of an entirety of the data set.

33. A decoder of content material comprising:

a renderer that is configured to receive:

an entirety parameter corresponding to the content material, and

a plurality of security identifiers upon which the entirety parameter is based, each security identifier corresponding to a data item of the content material,

an entirety checker, operably coupled to the renderer, that is configured to

determine an entirety value based on the plurality of security identifiers, and

preclude a rendering of the content material from the source in dependence upon a correspondence between the entirety value and the entirety parameter.

34. The decoder of claim 33, wherein

the renderer is further configured to receive the entirety parameter based on a random selection from a set of entirety parameters, each entirety parameter of the set of entirety parameters having an associated set of security identifiers.

35. The decoder of claim 33, wherein

the entirety parameter includes a hash value of a composite of the plurality of security identifiers.

36. The decoder of claim 33, wherein

the security identifier includes at least one of:

a watermark that is embedded in the corresponding data item

a hash value that is based on the corresponding data item.

37. The decoder of claim 36, wherein

the watermark includes:

a robust watermark that is configured such that a removal of the robust watermark causes a corruption of the corresponding data item, and

a fragile watermark that is configured such that a modification of the corresponding data item causes a corruption of the fragile watermark.

38. The decoder of claim 36, wherein

the entirety parameter includes a hash value of a composite of the watermarks corresponding to the plurality of security identifiers.

39. The decoder of claim 33, wherein the plurality of data items includes a plurality of at least one of: digitally encoded audio content, and digitally encoded video content.

40. The decoder of claim 33, wherein the entirety parameter is bound to a table of contents that is associated with the content material.